FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005-3315
202 • 408 • 4000
FACSIMILE 202 • 408 • 4400

ATLANTA
404•653•6400
PALO ALTO
650•849•6600

WRITER'S DIRECT DIAL NUMBER:

TOKYO
011•813•3431•6943
BRUSSELS
011•322•646•0353

#4

ATTORNEY DOCKET NO. 04329.2231

Assistant Commissioner
for Patents
Washington, D.C. 20231

U.S. Patent Application for: Personal Authentication System and Portable Unit and Storage Medium Used Therefor
Inventors: Miki Yamada et al.
Serial No.: 09/506,377 Group Art Unit: 2766
Filed: February 18, 2000

CLAIM FOR PRIORITY

Sir:

Under the provisions of Section 119 of 35 U.S.C., applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 11-041564 filed February 19, 1999, for the above identified United States Patent Application.

In support of applicants claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, L.L.P

by: _____
Richard V. Burgujian
Reg. No. 31,744

Dated: **JUNE 06, 2000**

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 1999年 2月19日

出願番号
Application Number: 平成11年特許願第041564号

出願人
Applicant (s): 株式会社東芝

2000年 3月 3日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特2000-3012229

【書類名】　特許願

【整理番号】　A009900781

【提出日】　平成11年 2月19日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 11/00

G06K 7/00

【発明の名称】　個人認証システム、それに使用される携帯装置及び記憶媒体

【請求項の数】　6

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　山田　貢己

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　森尻　智昭

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　才所　敏明

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　個人認証システム、それに使用される携帯装置及び記憶媒体

【特許請求の範囲】

【請求項１】　耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行可能な個人認証装置とを備えた個人認証システムであって、

前記携帯装置は、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手段を有し、

前記個人認証装置は、

前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手段と、

前記復号手段により得られた登録情報と前記入力情報とを照合する照合手段とを備えたことを特徴とする個人認証システム。

【請求項２】　請求項１に記載の個人認証システムに使用される携帯装置であって、

前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、

前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記個人認証装置の鍵で暗号化して得られた暗号文とを夫々前記個人認証装置に与える前記暗号化手段と

を備えたことを特徴とする携帯装置。

【請求項３】　請求項１に記載の個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、

前記携帯装置内のコンピュータに、

前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手順を実行させ、

前記個人認証装置内のコンピュータに、

前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手順を実行させ、

前記復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させる

ためのプログラムを記憶したコンピュータ読取り可能な記憶媒体。

【請求項４】　耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行可能な一つ或いは複数の個人認証装置と、耐タンパー性を有し、前記携帯装置と前記各個人認証装置との間にて暗号化を含む転送処理を行なう固設部とを備えた個人認証システムであって、

前記携帯装置は、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第１暗号化手段を備え、

前記固設部は、

前記第１暗号化手段から与えられた暗号文を復号して登録情報を得る第１復号手段と、

前記第１復号手段により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第２暗号化手段とを備え、

前記各個人認証装置は、移動可能に配置され、

前記第２暗号化手段から送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第２復号手段と、

前記第２復号手段により得られた登録情報と前記入力情報とを照合する照合手段と

を備えたことを特徴とする個人認証システム。

【請求項５】　請求項４に記載の個人認証システムに使用される携帯装置であって、

前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、

前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記固設部の鍵で暗号化して得られた暗号文とを夫々前記固設部に与える前記第１暗号化手段と

を備えたことを特徴とする携帯装置。

【請求項６】　請求項４に記載の個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、

前記携帯装置内のコンピュータに、

前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第１暗号化手順を実行させ、

前記固設部のコンピュータに、

前記第１暗号化手順により与えられた暗号文を復号して登録情報を得る第１復号手順を実行させ、

前記第１復号手順により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第２暗号化手順を実行させ、

前記各個人認証装置のコンピュータに、

前記第２暗号化手順により送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第２復号手順を実行させ、

前記第２復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させる

ためのプログラムを記憶したコンピュータ読取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えばＩＣカードの如き携帯可能な装置を用いる個人認証システム、それに使用される携帯装置及び記憶媒体に係り、特に、盗聴による不正を阻止し得る個人認証システム、それに使用される携帯装置及び記憶媒体に関する。

【０００２】

【従来の技術】

一般に、個人の権限の正当性を認証する分野では、商取引でのクレジットカードや立入制限場所での入退室管理カードの如き、携帯可能なＩＤカードを持参した個人に関してその権限の正当性を認証するための個人認証システムが広く用いられている。

【０００３】

この種のＩＤカードとしては、通常、磁気カードが使用される。また最近では、半導体チップの内蔵により、高セキュリティ性と高機能とを持つＩＣカードが使用され始めている。このＩＣカードは、磁気カードに比べて内部情報の読出／書込が困難であるため、偽造や情報漏洩などの不正を防止可能である旨が期待される。

【０００４】

但し、このようなＩＣカードは、単に内部情報を保持する構成のとき、紛失や盗難により他人に不正使用されたり、紛失と偽って不正使用される形態の不正を防止することが困難である。

よって、係る不正を防止する観点から、ＩＣカードでは、内部に個人認証情報が登録された構成とされる。これにより、個人認証装置の照合部では、ＩＣカードから送信された個人認証情報と、別途、操作入力された入力情報とが照合され、ＩＣカードを持参した者の権限の正当性が判定される。なお、個人認証情報はパスワードのようなものでもよい。

【０００５】

【発明が解決しようとする課題】

しかしながら、以上のような個人認証システムでは、ＩＣカードと照合部との間の通信内容が盗聴されることにより、不正に個人認証情報が読出されて不正使用されるという可能性がある。

【０００６】

本発明は上記実情を考慮してなされたもので、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用を阻止し得る個人認証システム、それに使用される携帯装置及び記憶媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】

請求項１に対応する発明は、耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行

可能な個人認証装置とを備えた個人認証システムであって、前記携帯装置としては、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手段を有し、前記個人認証装置としては、前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手段と、前記復号手段により得られた登録情報と前記入力情報とを照合する照合手段とを備えた個人認証システムである。

【０００８】

また、請求項２に対応する発明は、請求項１に対応する個人認証システムに使用される携帯装置であって、前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記個人認証装置の鍵で暗号化して得られた暗号文とを夫々前記個人認証装置に与える前記暗号化手段とを備えた携帯装置である。

【０００９】

さらに、請求項３に対応する発明は、請求項１に対応する個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、前記携帯装置内のコンピュータに、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記個人認証装置に与える暗号化手順を実行させ、前記個人認証装置内のコンピュータに、前記暗号化手段から与えられた暗号文を復号して登録情報を得る復号手順を実行させ、前記復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体である。

【００１０】

また、請求項４に対応する発明は、耐タンパー性を有し、登録情報の記憶された携帯装置と、耐タンパー性を有し、前記携帯装置との間で通信が可能なとき、前記携帯装置内の登録情報と新規に入力される入力情報とに基づいて、個人認証を実行可能な一つ或いは複数の個人認証装置と、耐タンパー性を有し、前記携帯装置と前記各個人認証装置との間にて暗号化を含む転送処理を行なう固設部とを備えた個人認証システムであって、前記携帯装置としては、前記個人認証が実行

されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第１暗号化手段を備え、前記固設部としては、前記第１暗号化手段から与えられた暗号文を復号して登録情報を得る第１復号手段と、前記第１復号手段により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第２暗号化手段とを備え、前記各個人認証部としては、移動可能に配置され、前記第２暗号化手段から送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第２復号手段と、前記第２復号手段により得られた登録情報と前記入力情報とを照合する照合手段とを備えた個人認証システムである。

【００１１】

さらに、請求項５に対応する発明は、請求項４に対応する個人認証システムに使用される携帯装置であって、前記個人認証が実行されるとき、乱数を生成する乱数生成手段と、前記乱数生成手段により生成された乱数により前記登録情報を暗号化して得られた暗号文と前記乱数を前記固設部の鍵で暗号化して得られた暗号文とを夫々前記固設部に与える前記第１暗号化手段とを備えた携帯装置である。

【００１２】

また、請求項６に対応する発明は、請求項４に対応する個人認証システムに使用されるコンピュータ読取り可能な記憶媒体であって、前記携帯装置内のコンピュータに、前記個人認証が実行されるとき、前記登録情報を暗号化し、得られた暗号文を前記固設部に与える第１暗号化手順を実行させ、前記固設部のコンピュータに、前記第１暗号化手順により与えられた暗号文を復号して登録情報を得る第１復号手順を実行させ、前記第１復号手順により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出する第２暗号化手順を実行させ、前記各個人認証装置のコンピュータに、前記第２暗号化手順により送出された暗号文を予め設定された暗号鍵により復号して登録情報を得る第２復号手順を実行させ、前記第２復号手順により得られた登録情報と前記入力情報とを照合する照合手順を実行させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体である。

【００１３】

（作用）

従って、請求項１，３に対応する発明は以上のような手段を講じたことにより、携帯装置の暗号化手段が、個人認証が実行されるとき、登録情報を暗号化し、得られた暗号文を個人認証装置に与え、個人認証装置の復号手段が、暗号化手段から与えられた暗号文を復号して登録情報を得ると、照合手段が、復号手段により得られた登録情報と入力情報とを照合するので、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用を阻止することができる。

【００１４】

また、請求項４，６に対応する発明は、携帯装置の第１暗号化手段が、個人認証が実行されるとき、登録情報を暗号化し、得られた暗号文を固設部に与え、固設部としては、第１復号手段が、第１暗号化手段から与えられた暗号文を復号して登録情報を得ると、第２暗号化手段が、第１復号手段により得られた登録情報を予め設定された暗号鍵により暗号化し、得られた暗号文を送出し、各個人認証装置の第２復号手段が、第２暗号化手段から送出された暗号文を予め設定された暗号鍵により復号して登録情報を得ると、照合手段が、第２復号手段により得られた登録情報と入力情報とを照合するので、請求項１，３に対応する作用に加え、各個人認証装置の接続の変更や固設部の暗号鍵の交換の場合でも、個人認証装置の同一性を保証でき、安全性を保持することができる。

【００１５】

また、請求項２，５に対応する発明は、携帯装置において、乱数生成手段が、個人認証が実行されるとき、乱数を生成し、暗号化手段が、乱数生成手段により生成された乱数により登録情報を暗号化して得られた暗号文と乱数を個人認証装置又は固設部の鍵で暗号化して得られた暗号文とを夫々個人認証装置又は固設部に与えるので、請求項１，４に対応する作用に加え、登録情報の暗号化鍵の変更が容易で、盗聴などによる登録情報の漏洩を阻止でき、内部情報の漏洩による影響を最小限に抑制でき、暗号解読攻撃に対して防御性を向上させることができる。

【００１６】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照しながら説明する。具体的には、以下の各実施形態では、最近注目されてきたバイオメトリクス技術を考慮し、従来のパスワードに代えて、個人の生体データを用いた場合について述べる。なお、バイオメトリクスは、生体データを用いて人間を認識する技術であり、例えば指紋認識、音声認識、手書き署名認識、網膜走査認識、及び手の幾何学的認識（掌型や指の長さ等）などがその技術範囲に含まれる。但し、パスワードを用い、パスワードと入力データとを照合する構成としても各実施形態は有効である。

【００１７】

（第１の実施形態）

図１は本発明の第１の実施形態に係る個人認証システムの構成を示す模式図である。この個人認証システムは、耐タンパー性を有するＩＣカード１０と、耐タンパー性を有するセンサユニット２０との２種類を主要な構成要素として有している。

【００１８】

なお、耐タンパー性は、内部情報の盗み見や改ざんから防御する性質であり、例えば不正なアクセス時に内部情報が消去される等の周知の機能を付加することにより、実現可能となっている。

【００１９】

係る個人認証システムは、具体的には、演算処理や表示処理等の通常の計算機機能の他、挿入されたＩＣカード（携帯装置）１０に対して情報を読出／書込可能なリーダライタ機能、センサユニット２０並びに業務ソフトウェア３０を有するクライアント装置４０を備えている。なお、リーダライタ機能は、別体の装置として設けてもよい。このクライアント装置４０及びＩＣカード１０は、例えば磁気ディスク等の記憶媒体に記憶されたプログラムを読込み、このプログラムによって動作が制御されるコンピュータによって実現される。但し、ＩＣカード１０は、生体データの登録の際にプログラムが読込まれ、以後、そのプログラムに基づいて動作する。

【００２０】

ここで、ＩＣカード１０は、耐タンパー性を有し、生成データ記憶部１１、認証部１２、暗号鍵記憶部１３及び暗号化部１４を備えている。生体データ記憶部１１は、予め個人の生体データが読出可能に記憶されたものである。生体データとしては、例えば指紋データ、音声（声紋）データ、手書き署名データ、網膜パターンデータ、又は手の幾何学データなどが適宜使用可能となっている。なお、ＩＣカードは、プログラムの読込に限らず、予め設計されたファームウェアを用いて実現してもよい。

【００２１】

認証部１２は、センサユニット２０との間で相互認証を行うためのものであり、自己（ＩＣカード）の正当性を証明するための証明書１５と、センサユニット２０から送られる証明書を検証するための認証局の公開鍵Ｐａと、復号された内容を照合するための認証局名と、自己の秘密鍵Ｓｉとを有している。

【００２２】

証明書１５は、少なくともＩＣカードの公開鍵Ｐｉの値、証明書１５を発行した認証局名、及びＰｉの値と前記認証局名の組を認証局の秘密鍵Ｓａでデジタル署名した署名の３つを有する。

【００２３】

認証部１２は、具体的には、ＩＣカード１０がクライアント装置４０に挿入されたとき、センサユニット２０の証明書を検証する機能と、センサユニット２０に関してセンサユニット２０の秘密鍵Ｓｓを有する旨を認証する機能と、センサユニット２０からＩＣカード１０の秘密鍵Ｓｉを有する旨を認証されるための機能とをもっている。

【００２４】

認証部１２において、センサユニット２０の証明書を検証する機能は、証明書１５をセンサユニット２０に送出する機能と、センサユニット２０から受けた証明書を認証局の公開鍵Ｐａを用いて検証し、復号結果を認証局名を用いて真偽判定する機能とからなる。

【００２５】

認証部１２において、センサユニット２０にてその秘密鍵Ｓｓを有する旨を認

証する機能は、証明書の検証における判定結果が“真”のとき、新規に暗号鍵Ｒ（疑似乱数）を生成する機能と、その暗号鍵Ｒをセンサユニット２０の証明書から得たセンサユニット２０の公開鍵Ｐｓで暗号化し、得られた暗号文Ｐｓ［Ｒ］をセンサユニット２０に送出する機能と、センサユニット２０から受けた暗号文Ｐｉ［Ｒ］を自己の秘密鍵Ｓｉで復号して得られた暗号鍵Ｒを自己の送出した暗号鍵Ｒに一致するか否かを判定する機能とからなり、判定結果が“真”のとき、その暗号鍵Ｒを暗号鍵記憶部１３に書込むようにしている。

【００２６】

なお、暗号鍵Ｒは、疑似乱数に限らないが、過去にその都度生成した暗号鍵Ｒによる暗号文Ｒ［Ｄ］の集合から予測不可能とする観点により疑似乱数が好ましい。

【００２７】

認証部１２において、センサユニット２０から自己が秘密鍵Ｓｉをもつ旨を認証される機能は、センサユニット２０から受けたメッセージＭ１を含む返信Ｍ１＋Ｍ２を作成し、Ｍ１＋Ｍ２を自己の秘密鍵Ｓｉにて署名した署名Ｓｉ［Ｍ１＋Ｍ２］，自己の証明書１５と共に乱数Ｒで暗号化してＲ［Ｍ１＋Ｍ２＋Ｓｉ［Ｍ１＋Ｍ２］＋証明書１５］を作成し、センサユニット２０の証明書から得たセンサユニット２０の公開鍵ＰｓでＲを暗号化したＰｓ［Ｒ］と共にセンサユニットに送出する機能とからなる。なお、Ｒ［Ｍ１＋Ｍ２＋Ｓｉ［Ｍ１＋Ｍ２］＋証明書１５］＋Ｐｓ［Ｒ］を以後、デジタル封書ＤＥ［Ｍ１＋Ｍ２，Ｓｉ，Ｐｓ；Ｒ］と呼ぶ。

【００２８】

暗号鍵記憶部１３は、暗号鍵Ｒが暗号化部１４から読出可能に記憶されるものである。

【００２９】

暗号化部１４は、生体データ記憶部１１内の生体データＤを暗号鍵記憶部１３内の暗号鍵Ｒにより暗号化してなる暗号文Ｒ［Ｄ］をセンサユニット２０内の復号部２３に送出する機能をもっている。

【００３０】

センサユニット２０は、耐タンパー性を有し、認証部２１、復号鍵記憶部２２、復号部２３、センサ２４、照合部２５及び演算部２６を備えている。

【００３１】

ここで、認証部２１は、ＩＣカード１０との間で相互認証を行うためのものであり、自己（センサユニット）の正当性を証明するための証明書２７と、ＩＣカード１０から送られる証明書１５を検証するための認証局の公開鍵Ｐａと、復号された内容を照合するための認証局名と、自己の秘密鍵Ｓｓとを有している。ここで、証明書２７は、少なくともセンサユニット２０の公開鍵Ｐｓの値、証明書２７を発行した認証局名、及びＰｓの値と前記認証局名の組を認証局の秘密鍵Ｓａでデジタル署名した署名の３つを有する。

【００３２】

認証部２１は、具体的には、ＩＣカード１０がクライアント装置４０に挿入されたとき、ＩＣカード１０の証明書１５を検証する機能と、ＩＣカード１０に関してＩＣカード１０の秘密鍵Ｓｉを有する旨を認証する機能と、ＩＣカード１０からセンサユニット２０の秘密鍵Ｓｓを有する旨を認証されるための機能とをもっている。

【００３３】

認証部２１において、ＩＣカード１０の証明書１５を検証する機能は、証明書２７をＩＣカード１０に送出する機能と、ＩＣカード１０から受けた証明書１５を認証局の公開鍵Ｐａを用いて復号し、復号結果を認証局名を用いて真偽判定する機能とからなる。

【００３４】

認証部１２において、ＩＣカード１０にてその秘密鍵Ｓｉを有する旨を認証する機能は、毎回異なるような（例えば乱数、時刻などを含む）メッセージＭ１を作成し、Ｍ１をＩＣカード１０に送出する機能と、ＩＣカード１０から受けたデジタル封書ＤＥ［Ｍ１＋Ｍ２，Ｓｉ，Ｐｓ；Ｒ］を自己の秘密鍵Ｓｓで復号して得られたメッセージＭ１が自己の送出したＭ１に一致するか否かを判定する機能と、デジタル封書［Ｍ１＋Ｍ２，Ｓｉ，Ｐｓ；Ｒ］に含まれる証明書１５の判定結果が“真”のとき、デジタル封書［Ｍ１＋Ｍ２，Ｓｉ，Ｐｓ；Ｒ］に含まれる

署名Ｓｉ［Ｍ１＋Ｍ２］がＩＣカード１０が署名したものであることを検証する機能とからなり、Ｍ１の判定結果が“真”で、且つ、ＩＣカード１０が署名したことを検証できたとき、ＩＣカード１０の認証処理を終了し、“偽”、又は、検証できなかったとき、エラー表示信号を発生して処理を終了するようにしている。

【００３５】

認証部２１において、ＩＣカード１０からセンサユニット２０の秘密鍵Ｓｓを有する旨を認証される機能は、ＩＣカード１０から受けた暗号文Ｐｓ［Ｒ］を自己の秘密鍵Ｓｓで復号し、得られた暗号鍵ＲをＩＣカード１０の証明書から得たＩＣカード１０の公開鍵Ｐｉで暗号化し、得られた暗号文Ｐｉ［Ｒ］をＩＣカード１０に送出する機能と、その暗号鍵Ｒを復号鍵記憶部２２に書込む機能とをもっている。

【００３６】

復号鍵記憶部２２は、認証部２１から書込まれた暗号鍵Ｒを復号部２３から読出可能に記憶するものである。

【００３７】

復号部２３は、ＩＣカード１０の暗号化部１４から暗号文Ｒ［Ｄ］を受けると、復号鍵記憶部２２内の暗号鍵Ｒにより暗号文Ｒ［Ｄ］を復号し、得られた生体データＤを照合部２５に与える機能をもっている。

【００３８】

センサ２４は、ユーザ（ＩＣカード携帯者）の生体測定を行ない、測定結果を電子化して生体測定データＤｍを作成してこの生体測定データＤｍを照合部２５に与える機能をもっている。

【００３９】

照合部２５は、センサ２４から受けた生体測定データＤｍと復号部２３から受けた生体データＤとを照合し、両者が一致したとき、許可データを演算部２６に与える機能と、両者が不一致のとき、エラー表示信号を発生する機能とをもっている。なお、センサ２４及び照合部２５は、指紋照合装置や掌型照合装置などが適宜使用可能となっている。

【００４０】

演算部２６は、照合部２５から受けた許可データを演算し、得られた結果データを業務ソフトウェア３０に与える機能をもっている。

業務ソフトウェア３０は、演算部２６から結果データを受けると実行可能となる任意の内容のアプリケーションであり、例えば会計処理用プログラムやプラント制御用プログラムといった任意の計算機ソフトウェアが使用可能である。

【００４１】

次に、以上のように構成された個人認証システムの動作を図２のフローチャートを用いて説明する。なお、ここでは、会社のクライアント／サーバシステム上の業務ソフトウェア３０を起動して端末業務を開始する際に、ＩＣカード１０によりユーザを確認する場合を例に挙げて述べる。

クライアント装置４０は、ユーザの操作により電源が投入され、コマンドやユーザＩＤの入力要求等の指示を画面表示し、ＩＣカード１０の挿入を待つ。

続いて、クライアント装置４０では、ユーザによりＩＣカード１０が挿入されると（ＳＴ１）、ＩＣカード１０とセンサユニット２０との夫々の認証部１２，２１が証明書の検証と、相互に秘密鍵を有する旨を認証する相互認証とを実行する（ＳＴ２）。

【００４２】

ステップＳＴ２の相互認証を、具体的に、認証手順を示した図３を用いて説明する。

【００４３】

センサユニット２０の認証部２１は、ＩＣカード１０がクライアント装置４０に挿入されたとき、証明書２７と、毎回異なるような（例えば乱数、時刻などを含む）メッセージＭ１とをＩＣカード１０に送出する（ＳＴ２１）。Ｍ１はＩＣカード１０の認証に用いられる。

【００４４】

次に、ＩＣカード１０の認証部１２は、センサユニット２０から受けた証明書２７に含まれる認証局の署名を認証局の公開鍵Ｐａを用いて復号し、この復号結果を認証局名を用いて真偽判定し、判定結果が“真”のとき、証明書２７の検証

を完了する（ＳＴ２２１）。

【００４５】

次に、ＩＣカード１０の認証部１２は、メッセージＭ１に対する返信Ｍ１＋Ｍ２を作成し（ＳＴ２２２）、新規に暗号鍵Ｒを作成し（ＳＴ２２３）、証明書１５を含むデジタル封書ＤＥ［Ｍ１＋Ｍ２，Ｓｉ，Ｐｓ；Ｒ］を作成し、センサユニットに送出する（ＳＴ２２４）。

【００４６】

次に、センサユニット２０の認証部２１は、ＩＣカード１０から受けたデジタル封書ＤＥ［Ｍ１＋Ｍ２，Ｓｉ，Ｐｓ；Ｒ］を自己の秘密鍵Ｓｓを用いて復号してＭ１＋Ｍ２と署名Ｓｉ［Ｍ１＋Ｍ２］とＩＣカード１０の証明書１５と暗号鍵Ｒとを取得し（ＳＴ２３１）、証明書１５に含まれる認証局の署名を認証局の公開鍵Ｐａを用いて復号し、この復号結果を認証局名を用いて真偽判定し、判定結果が“真”のとき、証明書１５の検証を完了する（ＳＴ２３２）。

【００４７】

なお、いずれの認証部１２，２１においても真偽判定の結果が“偽”を示すとき、エラー表示信号を発生して処理を終了する。

【００４８】

次に、センサユニット２０の認証部２１は、ＩＣカード１０の署名Ｓｉ［Ｍ１＋Ｍ２］を証明書１５から得られるＩＣカード１０の公開鍵Ｐｉで復号し、復号結果をＭ１＋Ｍ２、あるいはＭ１＋Ｍ２のメッセージダイジェストを用いて真偽判定し、また、センサユニットから受けたＭ１が自己の作成したＭ１と一致するか否かを真偽判定し、これら２つの判定結果が共に“真”のとき、ＩＣカード１０に関して、ＩＣカード１０の秘密鍵Ｓｉを有し、且つ、現在クライアント装置４０に接続されている旨の認証を完了し、暗号鍵Ｒを復号鍵記憶部２２に書込む。また、２つの判定結果のいずれかが“偽”のとき、エラー表示信号を発生して処理を終了する（ＳＴ２３３）。

【００４９】

次に、センサユニット２０の認証部２１は、暗号鍵ＲをＩＣカード１０の公開鍵Ｐｉで暗号化し、得られた暗号文Ｐｉ［Ｒ］ををＩＣカード１０に送出する（

ＳＴ２３４）。

【００５０】

次に、ＩＣカード１０の認証部１２は、センサユニット２０から受けた暗号文Ｐｉ［Ｒ］を自己の秘密鍵Ｓｉで復号して得られた暗号鍵Ｒを自己の送出した暗号鍵Ｒに一致するか否かを判定し、判定結果“真”のとき、センサユニット２０に関して、センサユニット２０の秘密鍵Ｓｓを有し、且つ、現在クライアント装置４０に接続されている旨の認証を完了し、暗号鍵Ｒを暗号鍵記憶部１３に書込む。また、判定結果が“偽”のとき、エラー表示信号を発生して処理を終了する（ＳＴ２４）と共に、ステップＳＴ２の相互認証の手順を終了する（ＳＴ２）。

【００５１】

以上の相互認証の手順（ＳＴ２）は、互いの証明書を検証し合い、互いの認証を行い、暗号鍵Ｒを通信路に対して秘匿しつつ互いに共有することを行なう他の手順にて行ってもよい。

【００５２】

次に、両認証部１２，２１において、いずれも真偽判定の結果が“真”であり、相互認証が完了した場合について述べる。なお、この相互認証が完了した時点において、両認証部１２，２１では、結果的に、新規に生成した乱数Ｒを共有しており、乱数Ｒを暗号用の鍵として使用可能としている。但し、相互認証の後、別に暗号鍵を生成してＩＣカード１０からセンサユニット２０に送出してもよい。

【００５３】

次に、ＩＣカード１０において、暗号化部１４は、生体データ記憶部１１内の生体データＤを暗号鍵記憶部１３内の暗号鍵Ｒにより暗号化し、得られた暗号文Ｒ［Ｄ］をセンサユニット２０内の復号部２３に与える（ＳＴ３）。

【００５４】

センサユニット２０においては、復号部２３がこの暗号文Ｒ［Ｄ］を受けると、復号鍵記憶部２２内の暗号鍵Ｒにより暗号文Ｒ［Ｄ］を復号し（ＳＴ４）、得られた生体データＤを照合部２５に与える。

【００５５】

センサ２４は、ユーザの指紋等の生体測定を行なう。生体測定は、例えば指紋を測定する場合、測定面上にユーザの指が乗せられて実行される。またセンサ２４では、生体の測定信号が入力されると（ＳＴ５）、その生体測定の結果を電子化して生体測定データＤｍを作成し、この生体測定データＤｍを照合部２５に与える。

【００５６】

照合部２５は、この生体測定データＤｍと復号部２３から受けた生体データＤとを照合して本人か否かを判定し（ＳＴ６）、両データＤ，Ｄｍが不一致のとき、“否”と判定してエラー表示信号を発生するが、両データＤ，Ｄｍの一致により“本人”と判定されたとき、許可データを演算部２６に与える。

【００５７】

演算部２６は、この許可データを演算し（ＳＴ７）、得られた結果データを業務ソフトウェア３０に与える。業務ソフトウェア３０は、演算部２６から結果データを受けることにより、実行が開始される。

【００５８】

上述したように本実施形態によれば、ＩＣカード１０の暗号化部１４が、個人認証が実行されるとき、生体データＤを暗号化し、得られた暗号文Ｒ［Ｄ］をセンサユニット２０に与え、センサユニット２０の復号部２３が、暗号文Ｒ［Ｄ］を復号して生体データＤを得ると、照合部２５が、この得られた生体データＤと入力された生体測定データＤｍとを照合するので、ＩＣカード１０とセンサユニット２０との間が盗聴されても、暗号文のために盗聴内容から情報を読出せず、その不正使用を阻止することができる。

【００５９】

また、ＩＣカード１０において、認証部１２が暗号鍵Ｒ（疑似乱数）を生成し、暗号化部１４が、その暗号鍵Ｒをセンサユニット２０の公開鍵Ｐｓの鍵で暗号化して得られた暗号文Ｐｓ［Ｒ］と、その暗号鍵Ｒにより生体データＤを暗号化して得られた暗号文Ｒ［Ｄ］とを夫々センサユニット２０に与えるので、生体データＤの暗号化鍵Ｒを容易に変更できることから、頻繁に暗号鍵Ｒを変更することにより、盗聴などによる生体データＤの漏洩やソフトウェア置換えによる不正

コマンド実行を阻止でき、暗号解読攻撃に対して防御性を向上させることができる。

【００６０】

また、ＩＣカード１０とセンサユニット２０とは相互認証を行うので、個人認証の確実性を向上させることができる。

【００６１】

例えば、ステップＳＴ２の手順を採らずに、通常のデジタル封書処理（乱数で本文と署名と証明書を暗号化し、さらにその乱数を相手の公開鍵で暗号化する）により、ＩＣカード１０から生体データＤをセンサユニット２０に送出するだけでも、毎回異なる鍵を利用して暗号文を送ることができることから、今回の発明と似た効果を得られる。

【００６２】

しかしながら、通常のデジタル封書処理では、その生体データＤが現在得られたものか否かの保証がない。すなわち、クライアント装置にて不正に置換されたソフトウェアがセンサユニット２０を騙そうとして、１週間前に得られたＩＣカード１０からの信号を保持しておき、その信号を今、センサユニット２０に送り込んだ場合でも、センサユニット２０がＩＣカード１０を現在挿入されていると判断してしまう問題がある。

【００６３】

これに対し、本実施形態では、乱数のやり取りを含む前述した相互認証を行うことにより、その瞬間にＩＣカード１０が挿入されていることと、その瞬間にセンサユニット２０が接続されていることとを確認できるので、より確実な本人確認を実行することができる。

【００６４】

また、毎回、ＩＣカード１０が暗号鍵Ｒを生成し、センサユニット２０に共有化させるので、特定のＩＣカード１０又はセンサユニット２０の内部情報が漏洩したとしても、他のＩＣカード１０又はセンサユニット２０の内部情報の連鎖的な漏洩を阻止することができる。

【００６５】

さらに、センサユニット２０の鍵ペア（公開鍵Ｐｓ－秘密鍵Ｓｓ）及びＩＣカード１０の暗号鍵Ｒを個別に更新できるので、便利で且つ暗号解読攻撃に対して強力な防御性を実現することができる。

【００６６】

また、バイオメトリクス技術を採用した場合、以上の効果に加え、パスワードを忘れたり、パスワードの書かれたメモを他人に読まれたり、といった可能性がないので、より一層、利便性を向上させることができる。

【００６７】

（第２の実施形態）

図４は本発明の第２の実施形態に係る個人検証システムの構成を示す模式図であり、図１と同一部分には同一符号を付してその詳しい説明を省略し、ここでは異なる部分について主に述べる。

【００６８】

本実施形態は、第１の実施形態の変形構成であり、複数のセンサユニット２０Ｂを接続可能として大規模化に対応した構成を示しており、クライアント装置４０が、センサユニット２０に代えて、耐タンパー性を有するクライアント認証部２０Ａと、耐タンパー性を有するセンサユニット２０Ｂとを備えている。

【００６９】

すなわち、この個人認証システムにおいて、耐タンパー性を有する構成要素は、ＩＣカード１０、クライアント認証部２０Ａ及びセンサユニット２０Ｂの３種類である。

【００７０】

ここで、クライアント認証部２０Ａは、ＩＣカード１０と相互認証を行い、ＩＣカード１０から受けた暗号文を復号してこの復号結果を共通鍵で暗号化し、この暗号文をセンサユニット２０Ｂに与える機能をもっている。

【００７１】

具体的には、クライアント認証部２０Ａは、耐タンパー性を有し、認証部２１、復号鍵記憶部２２、復号部２３ａ、共通鍵記憶部２８ａ、暗号化部２９を備えている。なお、認証部２１及び復号鍵記憶部２２は、前述同様の機能をもつもの

である。

【００７２】

復号部２３ａは、前述同様の復号機能を有し、得られた生体データＤを暗号化部２９に与える機能をもっている。

【００７３】

共通鍵記憶部２８ａは、図示しない管理ソフトウェアから与えられる共通鍵Ｃｋが暗号化部２９から読出可能に記憶されるものである。なお、管理ソフトウェアは、権限ある管理者のみが取扱うソフトウェアであり、クライアント装置４０Ａ内にあっても、他のサーバ装置（図示せず）内にあってもよい。

【００７４】

暗号化部２９は、復号部２３ａから受けた生体データＤを共通鍵記憶部２８ａ内の共通鍵Ｃｋにより暗号化し、得られた暗号文Ｃｋ［Ｄ］をセンサユニット２０Ｂ内の復号部２３ｂに与える機能をもっている。

【００７５】

センサユニット２０Ｂは、耐タンパー性を有し、共通鍵記憶部２８ｂ、復号部２３ｂ、センサ２４、照合部２５及び演算部２６を備えている。

共通鍵記憶部は、図示しない管理ソフトウェアから与えられる共通鍵Ｃｋが復号部から読出可能に記憶されるものである。

【００７６】

復号部２３ｂは、クライアント認証部２０Ａの暗号化部２９から暗号文Ｃｋ［Ｄ］を受けると、共通鍵記憶部２８ｂ内の共通鍵Ｃｋにより暗号文Ｃｋ［Ｄ］を復号し、得られた生体データＤを照合部２５に与える機能をもっている。

センサ２４、照合部２５及び演算部２６は、前述同様の機能をもつものである。

【００７７】

次に、以上のように構成された個人認証システムの動作を図５のフローチャートを用いて説明する。

ステップＳＴ１～ＳＴ４の復号処理までは、前述同様に行われる。

すなわち、クライアント装置４０Ａの復号部２３ａは、前述同様の復号機能を

有し、ＩＣカード１０の暗号化部１４から暗号文Ｒ［D］を受けると、復号鍵記憶部２２内の暗号鍵Ｒにより暗号文Ｒ［D］を復号する（ＳＴ４）。

【００７８】

但し、復号部２３ａは、得られた生体データＤを暗号化部２９に与える。

暗号化部２９は、復号部２３ａから受けた生体データＤを共通鍵記憶部２８ａ内の共通鍵Ｃｋにより暗号化して得られた暗号文Ｃｋ［D］をセンサユニット２０Ｂ内の復号部２３ｂに与える（ＳＴ４ａ）。

【００７９】

センサユニット２０Ｂでは、復号部２３ｂが、クライアント認証部２０Ａの暗号化部２９から暗号文Ｃｋ［D］を受けると、共通鍵記憶部２８ｂ内の共通鍵Ｃｋにより暗号文Ｃｋ［D］を復号し（ＳＴ４ｂ）、得られた生体データＤを照合部２５に与える。

【００８０】

以下、前述同様にステップＳＴ５～ＳＴ７が実行され、正当なユーザである場合、業務ソフトウェア３０の実行が開始される。

上述したように本実施形態によれば、複数のセンサユニット２０Ｂを有する場合であっても、各センサユニット２０Ｂとクライアント認証部２０Ａとを共通鍵方式により結合することにより、第１の実施形態の効果を得ることができ、さらに、各センサユニット２０Ｂの接続の変更やクライアント認証部２０Ａの暗号鍵の交換の場合でも、クライアント装置４０Ａの同一性を保証できるので、安全性を保持することができる。

【００８１】

また同様に、耐タンパー性をもつクライアント認証部２０Ａが認証処理を行なうので、複数のセンサユニット２０Ｂが接続されていたり、各センサユニット２０Ｂが着脱自在であっても、認証処理の安全性を確保することができる。

【００８２】

また、１つのクライアント認証部２０Ａが認証処理を行うことにより、複数のセンサユニット２０Ｂ及び複数のＩＣカード１０を有する大規模な構成の場合であっても、暗号鍵の更新の際に、クライアント認証部２０Ａの鍵ペア（公開鍵Ｐ

ｓ－秘密鍵Ｓｓ）のみを更新すれば、その更新した公開鍵Ｐｓを、相互認証の際にＩＣカード１０に伝送できるので、暗号鍵の更新が容易であり、便利である。

【００８３】

（他の実施形態）

なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に書込んで各種装置に適用したり、通信媒体により伝送して各種装置に適用することも可能である。

【００８４】

また、上記各実施形態では、照合部２５が演算部２６を介して結果情報を出力する場合について説明したが、これに限らず、演算部２６が、ＩＣカード１０の公開鍵Ｐｉを用いて演算結果を暗号化してＩＣカード１０に送出し、ＩＣカード１０がサーバ装置（図示せず）を介して業務ソフトウェア３０を起動する構成により、業務ソフトウェア３０の実行を開始する際に業務ソフトウェア３０には演算結果を秘匿する方式としても、本発明を同様に実施して同様の効果を得ることができる。

【００８５】

さらに、上記各実施形態では、２つの認証部１２，２１により証明書を利用した相互認証を行なう場合を説明したが、これに限らず、ＩＣカード１０とクライアント装置４０，４０Ａとに夫々共通鍵を持たせた共通鍵方式としても、本発明を同様に実施して同様の効果を得ることができる。

【００８６】

また、上記各実施形態では、ＩＣカード１０に生体データＤが保持され、クライアント装置４０，４０Ａにてセンサ２４から生体測定データＤｍが入力され、両データＤ，Ｄｍが照合される場合を説明したが、これに限らず、ＩＣカード１０にパスワード（ユーザ情報）が保持され、クライアント装置４０，４０Ａにて入力デバイス（キーボード又はタッチパネル等）からパスワード（ユーザ情報）が入力され、両パスワードが照合される方式としても、本発明を同様に実施して

同様の効果を得ることができる。

【００８７】

また、上記各実施形態では、携帯装置を、耐タンパー性を有するＩＣカード１０とした場合について説明したが、これに限らず、耐タンパー性を有して携帯可能なものであれば、携帯装置を、携帯電話や電子手帳等の任意の個人情報機器としても、本発明を同様に実施して同様の効果を得ることができる。また、携帯装置の性質に応じ、携帯装置とクライアント装置との間の通信を、無線又は赤外線（任意波長の光）等のような任意の通信方式に変形してもよい。

【００８８】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【００８９】

【発明の効果】

以上説明したように本発明によれば、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用を阻止し得る個人認証システム、それに使用される携帯装置及び記憶媒体を提供できる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係る個人認証システムの構成を示す模式図

【図２】

同実施形態における動作を説明するためのフローチャート

【図３】

同実施形態における相互認証の手順を説明するための概略図

【図４】

本発明の第２の実施形態に係る個人検証システムの構成を示す模式図

【図５】

同実施形態における動作を説明するためのフローチャート

【符号の説明】

１０…ＩＣカード

１１…生体データ記憶部

１２，２１…認証部

１３…暗号鍵記憶部

１４，２９…暗号化部

１５，２７…証明書

２０，２０Ｂ…センサユニット

２０Ａ…クライアント認証部

２２…復号鍵記憶部

２３，２３ａ，２３ｂ…復号部

２４…センサ

２５…照合部

２６…演算部

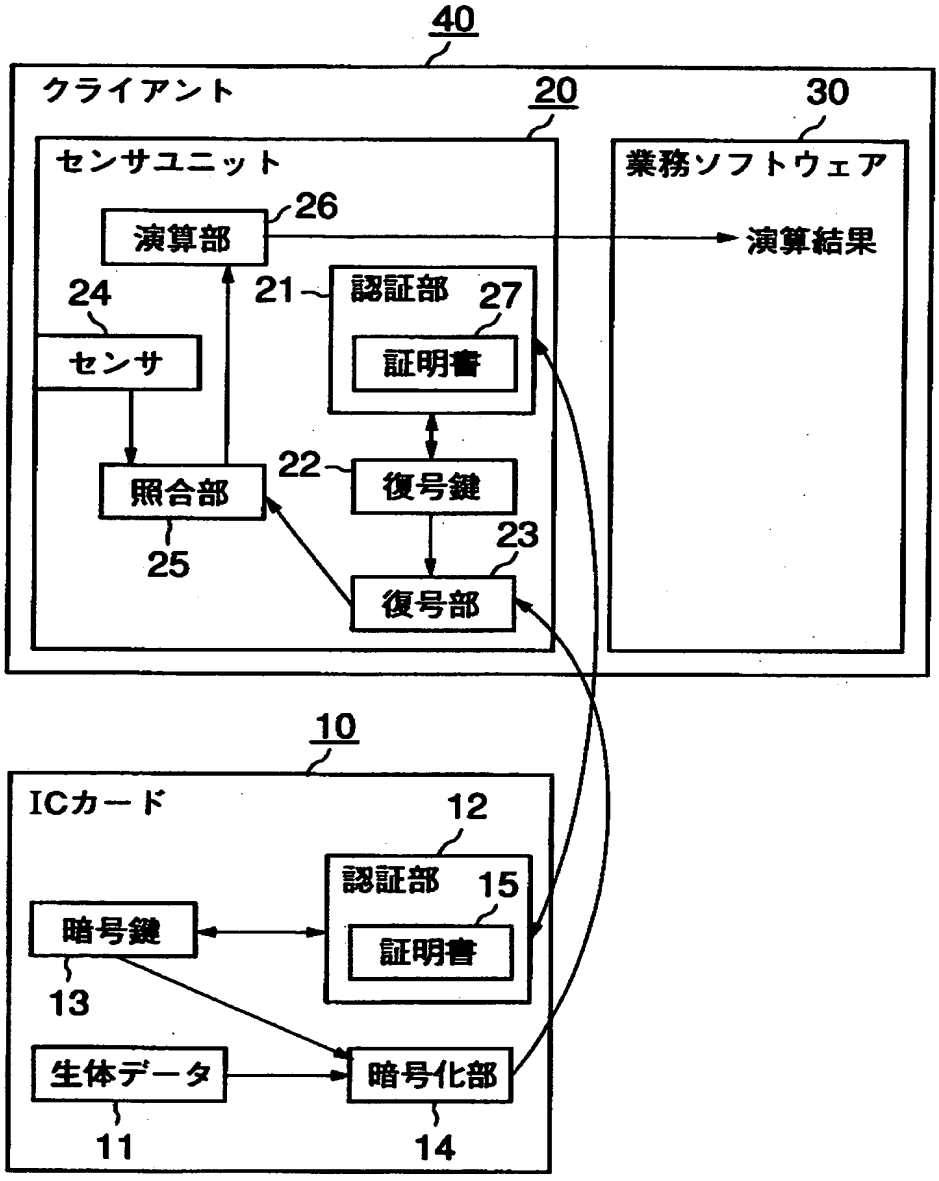
２８ａ，２８ｂ…共通鍵記憶部

３０…業務ソフトウェア

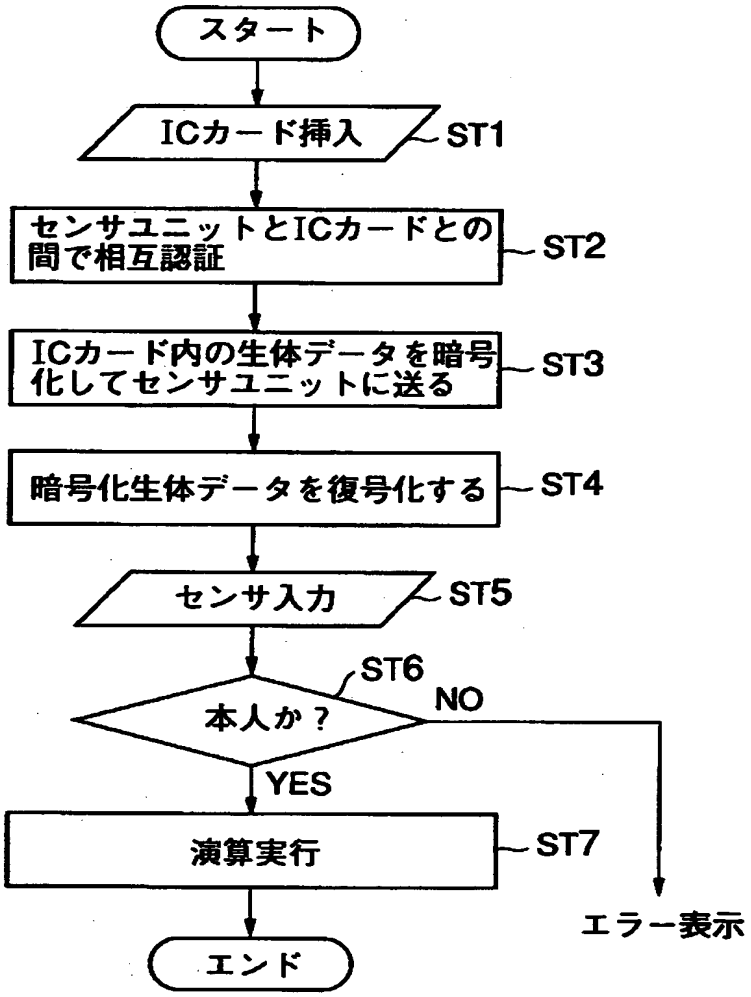
４０，４０Ａ…クライアント装置

【書類名】　　図面

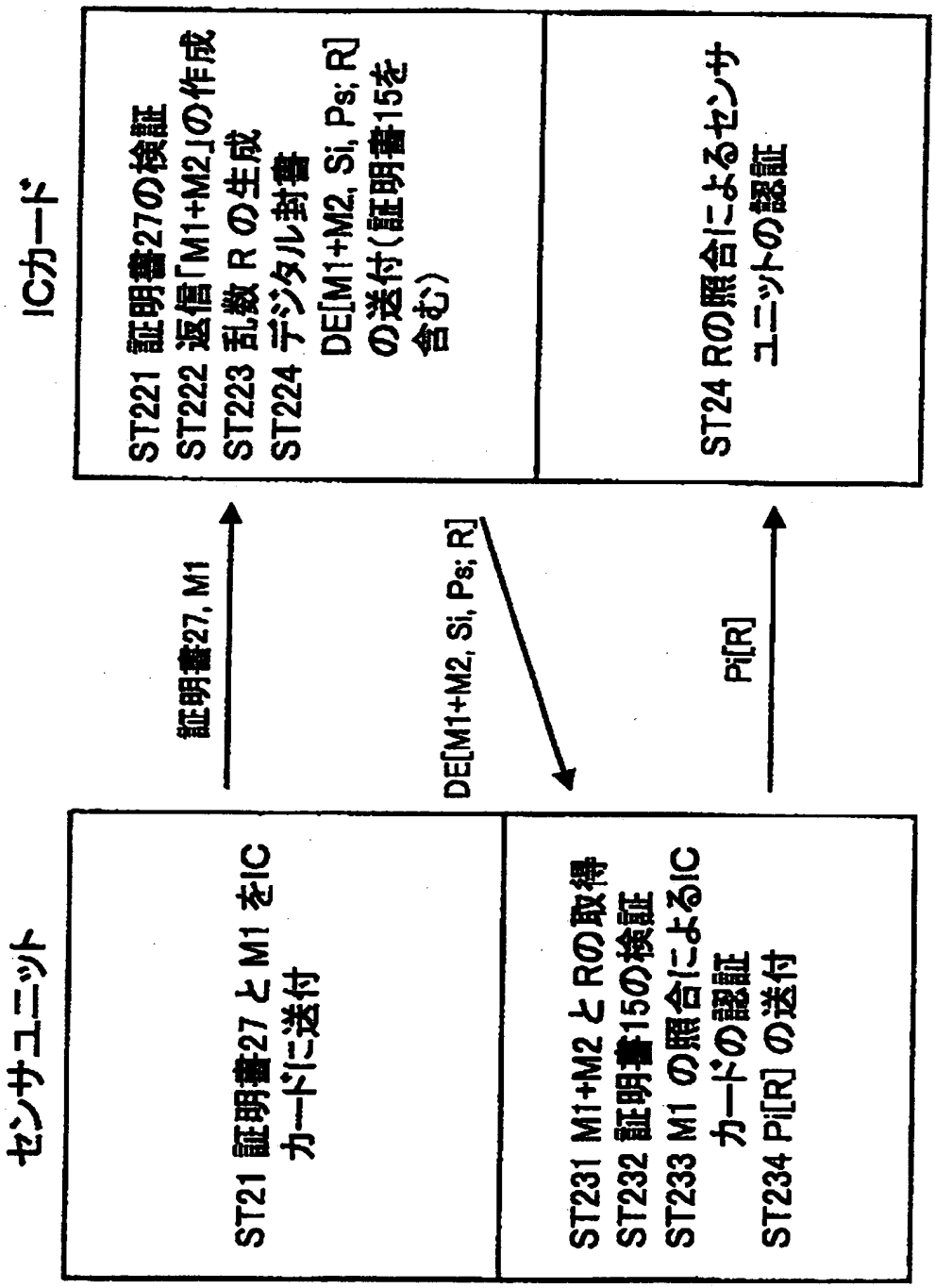
【図１】


40
クライアント
20
30
センサユニット
業務ソフトウェア
演算部
26
演算結果
24
21
認証部
27
センサ
証明書
22
照合部
復号鍵
25
23
復号部
10
ICカード
12
認証部
15
暗号鍵
証明書
13
生体データ
暗号化部
11
14

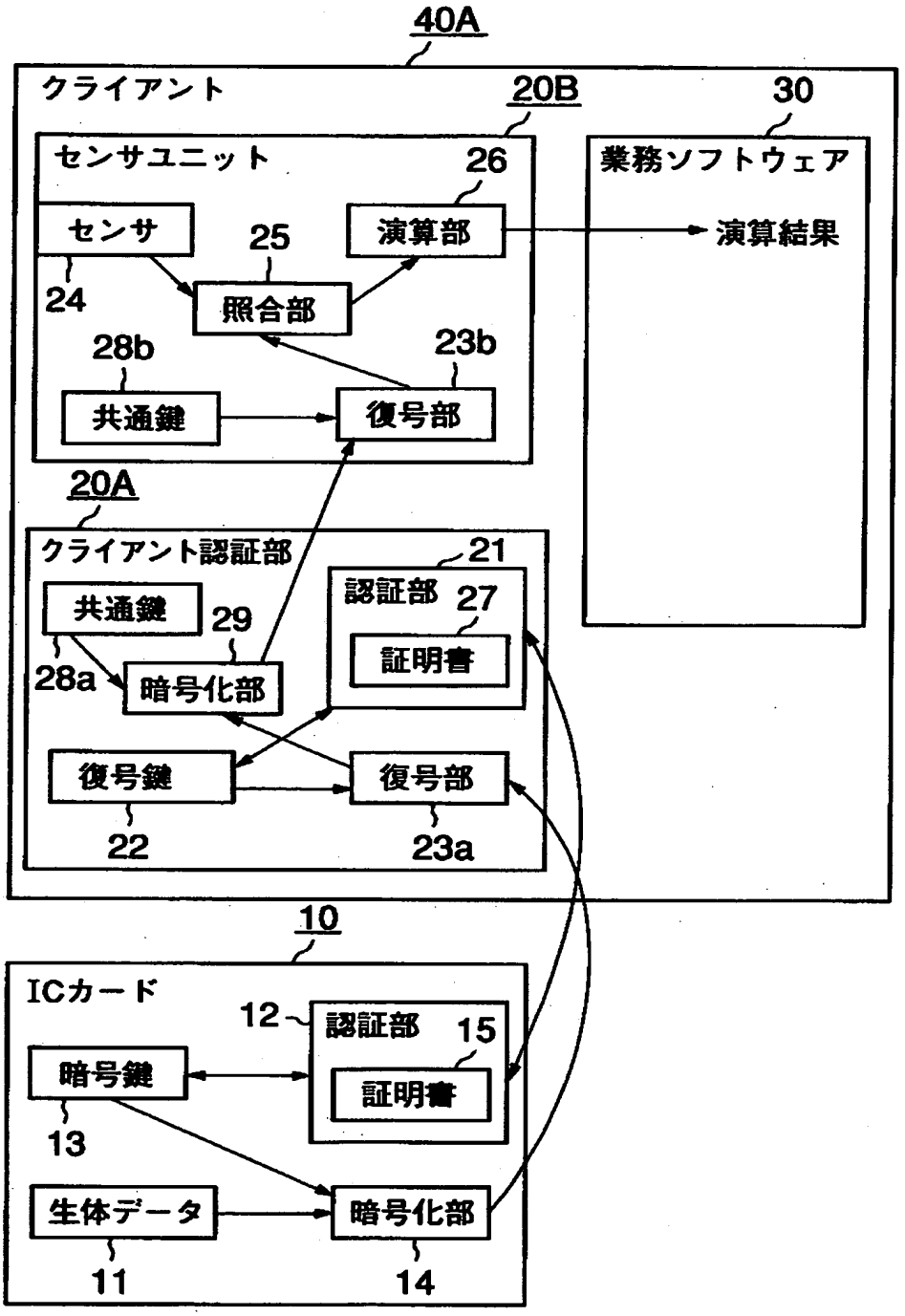
【図２】


スタート
ICカード挿入
ST1
センサユニットとICカードとの間で相互認証
ST2
ICカード内の生体データを暗号化してセンサユニットに送る
ST3
暗号化生体データを復号化する
ST4
センサ入力
ST5
ST6
本人か？
NO
YES
演算実行
ST7
エラー表示
エンド

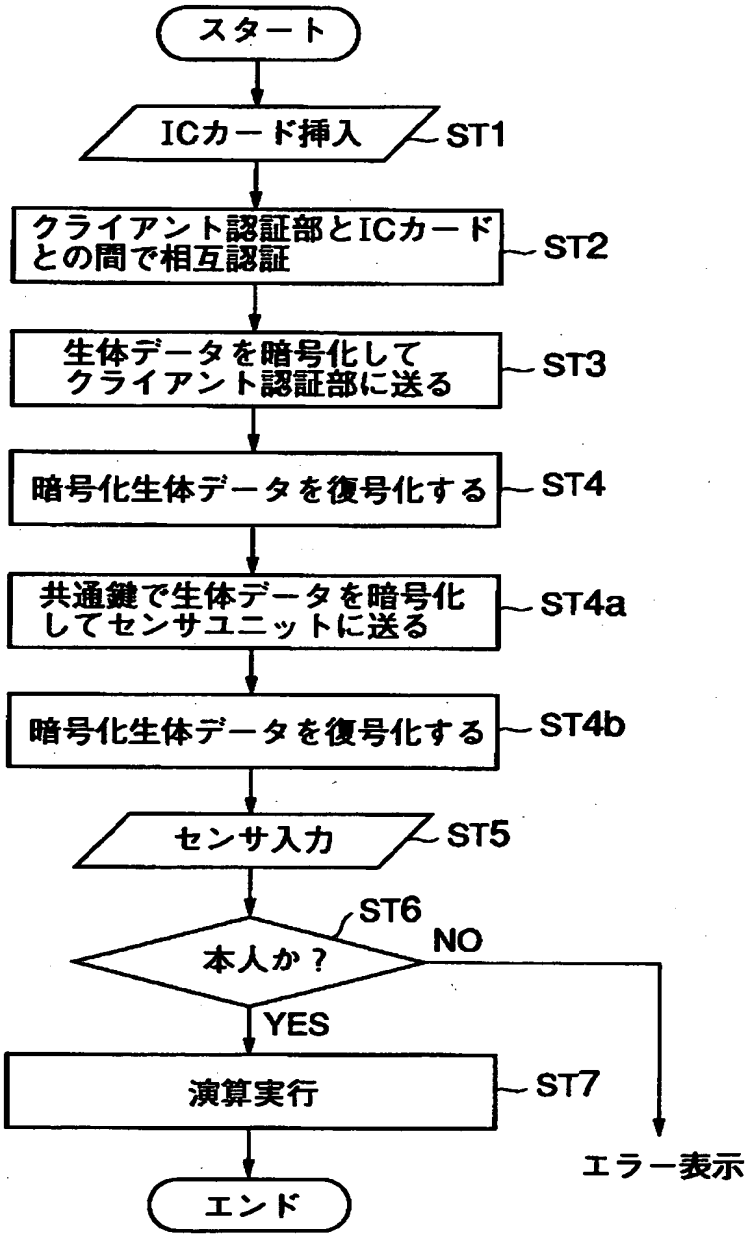
【図３】


ICカード
センサユニット
ST221 証明書27の検証
ST222 返信「M1+M2」の作成
ST223 乱数 R の生成
ST224 デジタル封書
DE[M1+M2, Si, Ps; R]
の送付(証明書15を
含む)
ST24 Rの照合によるセンサ
ユニットの認証
ST21 証明書27 と M1 をIC
カードに送付
ST231 M1+M2 と Rの取得
ST232 証明書15の検証
ST233 M1 の照合によるIC
カードの認証
ST234 Pi[R] の送付
証明書27, M1
DE[M1+M2, Si, Ps; R]
Pi[R]

【図４】


40A
クライアント
20B
30
センサユニット
26
業務ソフトウェア
センサ
25
演算部
演算結果
24
照合部
28b
23b
共通鍵
復号部
20A
クライアント認証部
21
共通鍵
29
認証部
27
28a
暗号化部
証明書
復号鍵
復号部
22
23a
10
ICカード
12
認証部
15
暗号鍵
証明書
13
生体データ
暗号化部
11
14

【図５】


スタート
ICカード挿入
ST1
クライアント認証部とICカードとの間で相互認証
ST2
生体データを暗号化してクライアント認証部に送る
ST3
暗号化生体データを復号化する
ST4
共通鍵で生体データを暗号化してセンサユニットに送る
ST4a
暗号化生体データを復号化する
ST4b
センサ入力
ST5
ST6
本人か？
NO
YES
演算実行
ST7
エラー表示
エンド

【書類名】　　要約書

【要約】

【課題】　本発明は、携帯装置と個人認証装置との間が盗聴されても、盗聴内容から情報を読出せず、その不正使用の阻止を図る。

【解決手段】　ＩＣカード１０の暗号化部１４が、個人認証が実行されるとき、生体データＤを暗号化し、得られた暗号文Ｒ［Ｄ］をセンサユニット２０に与え、センサユニット２０の復号部２３が、暗号文Ｒ［Ｄ］を復号して生体データＤを得ると、照合部２５が、この生体データＤと入力された生体測定データＤｍとを照合して本人か否かを判定する個人認証システム、それに使用される携帯装置及び記憶媒体。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝